SECURANCE

Vitpapper - ISAE 3402

Följsamhet mot ISAE 3402.

Innehåll

Att lära känna ISAE 3402

I detta vitpapper kommer vi att ge dig den nödvändiga informationen om ISAE 3402. Vitpapperet innehåller information om ISAE 3402-standarden, projektfaserna för ISAE 3402-efterlevnad (definiera omfattningen, implementeringen och revisionen), samt fördelarna med ISAE 3402 för din organisation.

Som en professionell rådgivare inom riskhantering, styrning och efterlevnad är vi glada att kunna stödja dig med ISAE 3402-efterlevnadsprojektet inom din organisation. Vi svarar gärna på eventuella frågor du kan ha angående ISAE 3402

ISAE 3402

Outsourcing | Säkerhet för finansiella processer

ISAE 3402 är en internationellt erkänd revisionsstandard eftersom den representerar en djupgående granskning av en tjänsteorganisations kontrollmål och kontrollaktiviteter, som ofta inkluderar kontroller över informationsteknik och relaterade processer.

Omfattningen av granskningen av den externa revisorn inkluderar de transaktionsklasser inom tjänsteorganisationens verksamhet som är betydande för användarorganisationens finansiella rapporter och processer som är specifikt definierade av tjänsteorganisationen. ISAE 3402 är allmänt tillämplig när en oberoende revisor ("användarrevisor") planerar finansiell revision av en enhet ("användarorganisationen") som får tjänster från en annan organisation ("tjänsteorganisationen").

Tjänsteorganisationens rapport, som inkluderar tjänsteorganisationens revisors utlåtande, utfärdas till tjänsteorganisationen vid avslutningen av en ISAE 3402-garantiuppdrag. ISAE 3402 specificerar inte en förutbestämd uppsättning kontrollmål eller kontrollaktiviteter som tjänsteorganisationer måste uppnå.

Outsourcing

Outsourcade tjänster kräver att tjänsteorganisationen hanterar de risker som är förknippade med dessa tjänster. En ISAE-rapport är en internkontrollrapport som tillhandahåller denna information. ISAE 3402 är standarden för garanti på finansiella processer (eller processer med finansiell påverkan för användarorganisationen).

De relevanta processerna, riskhanteringsramverket och en detaljerad kontrollmatris behöver beskrivas av en organisation. Den detaljerade kontrollmatrisen måste innehålla kontrollmål och kontrollbeskrivningar.

Efter implementeringen måste alla procedurer och kontroller vara på plats. Alla arbetsprocedurer, processhantering och disciplin inom organisationen kräver enhetlighet för att följa de beskrivna procedurerna i rapporten.

Industrier

Organisationer som tillhandahåller tjänster till andra organisationer, till exempel förvaltare av tillgångar/fastigheter, pensionsserviceleverantörer, programvara som en tjänst (SaaS)-leverantörer, infrastruktur som en tjänst (IaaS)-leverantörer, plattform som en tjänst (PaaS)-leverantörer och datacenter-tjänsteleverantörer, är i allmänhet skyldiga att genomföra en ISAE 3402-rapport.

Om outsourcade processer är relaterade till finansiella processer är ISAE 3402 relevant. En ISAE 3000- eller SOC 2-rapport kan vara mer relevant om processerna är relaterade till allmänna IT-kontroller (GITC), säkerhet och/eller integritet.

Fas 1. Omfattningsdefinition

Hur Definerar man Omfattningen av en ISAE 3402-rapport?

Omfattningen av en ISAE 3402-rapport som rör de finansiella kontrollerna inom en tjänsteorganisation är relevant för de finansiella processerna i relation till de tillhandahållna tjänsterna (eller processer med finansiell påverkan för användarorganisationen, om det inte görs några direkta finansiella transaktioner).

ISAE 3402-rapporten bör innehålla en omfattningssektion som noterar de viktiga komponenterna av omfattningen, inklusive de tjänsteleverantörer som ingår eller är undantagna. Det är nödvändigt att inkludera detaljer om typen av tillhandahållna tjänster, det interna kontrollramverket (baserat på COSO-ramverket) och en beskrivning av de allmänna IT-kontrollerna.

Förbered Omfattning

Grunden för att förbereda omfattningen av ISAE 3402-rapporten är outsourcingriskerna (finansiella, efterlevnadsrelaterade, operationella) för användarorganisationen. Risker i samband med ICT-strukturen bör också definieras inom detta sammanhang. För de relevanta processerna som är kopplade till de identifierade riskerna definieras specifika kontrollmål. Baserat på de förberedda kontrollmålen beskrivs kontrollerna för att uppnå kontrollmålen och i slutändan minska outsourcingriskerna. Den kompletterande användarorganisationens kontroll ger ytterligare detaljer om omfattningen, omfattningens gränser och de kontroller som måste finnas på plats i användarorganisationen.

I slutändan är det upp till ledningen att definiera omfattningen av en ISAE 3402-rapport, även om kravet är att de processer som kan ha en finansiell effekt för användarorganisationen åtminstone ska ingå.

Inkluderande eller Undantag?

Om en tjänsteorganisation (delvis) outsourcar sina processer, är detta en så kallad underleverantörsorganisation. Tjänsteorganisationen avgör om de relevanta kontrollerna för underleverantörsorganisationen beskrivs. ISAE 3402-riktlinjerna föreskriver två metoder för detta; undantagsmetoden och den inkluderande metoden.

Vid användning av undantagsmetoden bör det tydligt framgå i tjänsteorganisationens beskrivning att kontrollerna och kontrollmålen för underleverantörsorganisationen inte ingår i beskrivningen eller revisorns granskning av tjänsteorganisationen.

Vid användning av den inkluderande metoden anger tjänsteorganisationen att kontrollerna för underleverantörsorganisationen ingår i beskrivningen av kontrollerna. En undantagsmetod kan användas om underleverantörsorganisationen har en ISAE 3402 (SOC 1) eller SOC 2-rapport på plats.

Konkurrensfördel

Hur en ISAE 3402 Rapport Ger Dig en Fördel Framför Dina Konkurrenter

ISAE 3402 erbjuder en konkurrensfördel genom att särskilja tjänsteorganisationer från deras konkurrenter. Fördelarna med ISAE 3402-rapporter sträcker sig från förstärkning och förfining av riskhantering till att skapa förtroende på marknader genom transparens i kontrollramverket.

FAS 2. Implementering

Steg-för-steg Tillvägagångssätt

1. Konsekvensanalys & Omfattning

I Fas 1 bestäms effekten (GAP-analys) av implementeringen. Baserat på effekten och den definierade omfattningen av implementeringen, förbereds en detaljerad plan där olika milstolpar identifieras och arrangemang med ledningen görs.

2. Processer & Kontroller

I Fas 2 hålls intervjuer för att identifiera risker, bestämma effekten och den befintliga arbetsmetoden, samt att notera den information som finns inom organisationen. Organisationens kontrollåtgärder beskrivs sedan enligt ISAE 3402-kraven baserat på den information som erhållits från intervjuerna. Dessa registreras i en kontrollmatris; en matris som innehåller kontrollmål och relaterade kontroller. Vi kommer att ge proaktiv rådgivning om implementeringen av eventuella saknade kontroller (inklusive processbeskrivningar).

3. Kontrollramverk

I Fas 3 kommer det interna kontrollramverket att beskrivas baserat på det senaste COSO-ramverket (COSO 2013) och den allmänna sektionen om rapporteringen förbereds. I den allmänna sektionen ingår en beskrivning av processerna, organisationen och de allmänna IT-kontrollerna.

4. ISAE 3402 Rapport

I Fas 4 förbereds den kompletta ISAE 3402-rapporten baserat på de individuella sektionerna och tilläggssektioner såsom ledningsuttalandet och de kompletterande användarorganisationens kontroller. Fas 4 resulterar i ett utkast till ISAE 3402-rapporten. Vi kommer att diskutera denna rapport i detalj med relevant personal. Organisationen kommer att implementera eventuella identifierade saknade kontroller under denna fas.

Handläggningstiden för de första fyra faserna kommer att vara mellan sex och åtta veckor, beroende på engagemanget och tillgängligheten av medarbetare. Den förväntade tillgängligheten av medarbetare är en dag per vecka under den perioden.

5. Förrevision

Efter förberedelsen av rapporten kommer Securance att genomföra en förrevision eller "walkthrough" i Fas 5. Under förrevisionen kommer kontrollåtgärderna att testas, och eventuella problemområden kommer att identifieras innan den slutliga revisionen. Under denna fas kommer organisationen att tillhandahålla den dokumentation och bevis som krävs av Securance.

6. Åtgärder

Under Fas 6, som ett resultat av förrevisionen, implementeras förbättringar av kontrollåtgärder och ledningssystemet och lösningar för de identifierade problemområdena förbereds. Securance kommer att ge lösningar som kan implementeras inom organisationen och i ISAE 3402-rapporten. Fas 6 kommer att resultera i den slutliga ISAE 3402-rapporten.

Handläggningstiden för faserna 5 och 6 är mellan två och fyra veckor. Den förväntade tillgängligheten av medarbetare är en dag per vecka under den perioden.

Definiera Kontroller

Förklaringar av Kontrolltyper

Ett kontrollramverk består alltid av allmänna IT-kontroller, manuella kontroller och övervakningskontroller. Dessa kontroller tillsammans bildar det kontrollramverk med vilket risker hanteras.
Övervakningskontroller fungerar som ett sekundärt 'filter' för oegentligheter som inte har upptäckts av de primära ledningskontrollerna. Det interna kontrollramverket består alltid av en uppsättning kontroller; kontroller som arbetar tillsammans. Denna uppsättning kontroller säkerställer att risker kontrolleras effektivt.

Allmänna IT-Kontroller

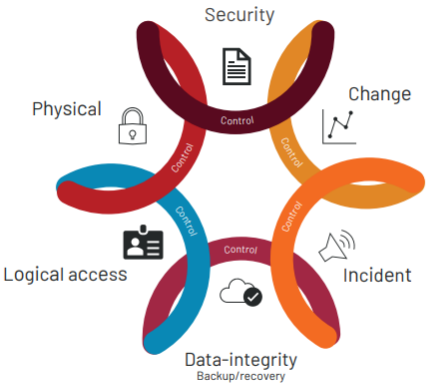
De allmänna IT-kontrollerna är de kontroller som säkerställer att det finns tillräckliga säkerhets- och dataintegritetsåtgärder för att säkerställa att finansiell information är korrekt och komplett för syftet med de finansiella rapporterna. Ett internationellt erkänt ramverk för de allmänna IT-kontrollerna är COBIT 5.0-ramverket.

Applikationskontroller

Applikationskontroller är automatiserade kontroller inom ett system eller en applikation som är upprättade (t.ex. genom ett skript) och som kan garantera bland annat fullständigheten och integriteten av in-och utmaningsdata, auktorisering och autentisering av data och användare, samt tillgänglighet av system.

Manuella Kontroller

Manuella kontroller är de kontroller som utförs av en auktoriserad individ inom användarorganisationen. Detta kan variera från testning av mjukvarureleaser till auktorisering av finansiella transaktioner i den finansiella administrationen eller auktorisering av säkerhetskopieringsrapporter. Applikationskontrollerna stödjer de manuella kontrollerna.



Övervakningskontroller

ISAE 3402-riktlinjerna föreskriver inte uttryckligen enhetsnivåkontroller eller övervakningskontroller. Det är dock god praxis att beskriva övervakningskontroller i ISAE 3402-rapporten. Idealiskt sett är företagsnivåkontrollerna i linje med COSO-ramverket. Andra övervakningskontroller ingår i kontrollmatrisen per process.

FAS 3. Revision

Kvalitetssäkringsrevisioner

ISAE 3402 Revision

En ISAE 3402-rapport gör det möjligt för tjänsteorganisationer att avslöja sina kontrollaktiviteter och processer för sina kunder och deras kunders revisorer i ett enhetligt rapporteringsformat. Tjänsterevisorns rapport, som inkluderar tjänsterevisorns utlåtande, utfärdas till tjänsteorganisationen vid avslutningen av revisionen.

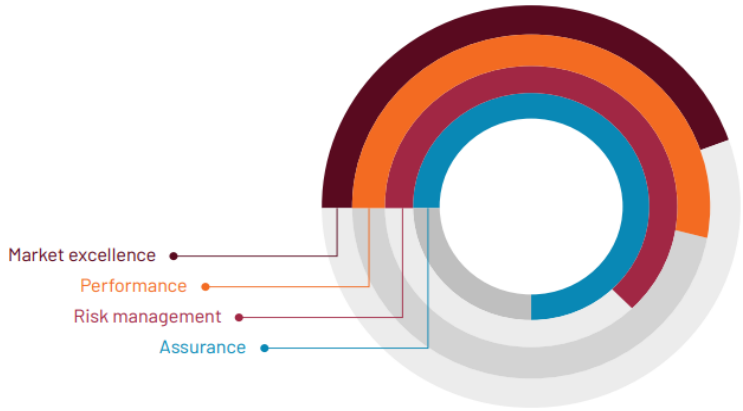
ISAE 3402 specificerar inte en förutbestämd uppsättning kontrollmål eller kontrollaktiviteter som tjänsteorganisationer måste uppnå. Att identifiera och utvärdera relevanta kontroller är i allmänhet ett viktigt steg i användarrevisorns övergripande metod för revision av finansiella rapporter. En tjänsterevisor kan utfärda två typer av rapporter: en Typ I-rapport eller en Typ II-rapport.

Typ I Rapport

En ISAE 3402 Typ I-rapport inkluderar en åsikt från en extern revisor om de kontroller som har satts i drift vid en specifik tidpunkt. Den externa revisorn undersöker huruvida kontrollerna är lämpligt utformade för att ge rimlig säkerhet om att de finansiella rapporteringspåståendena är uppfyllda och om kontrollerna är på plats.

Typ II Rapport

I en ISAE 3402 Typ II-rapport rapporterar den externa revisorn om lämpligheten av designen och förekomsten av kontroller samt om den operativa effektiviteten hos dessa kontroller under en fördefinierad period på minst sex månader. Detta innebär att den externa revisorn utför en detaljerad granskning av de interna kontrollerna hos tjänsteorganisationen och också undersöker om alla kontroller fungerar effektivt i enlighet med de fördefinierade processerna och kontrollerna.

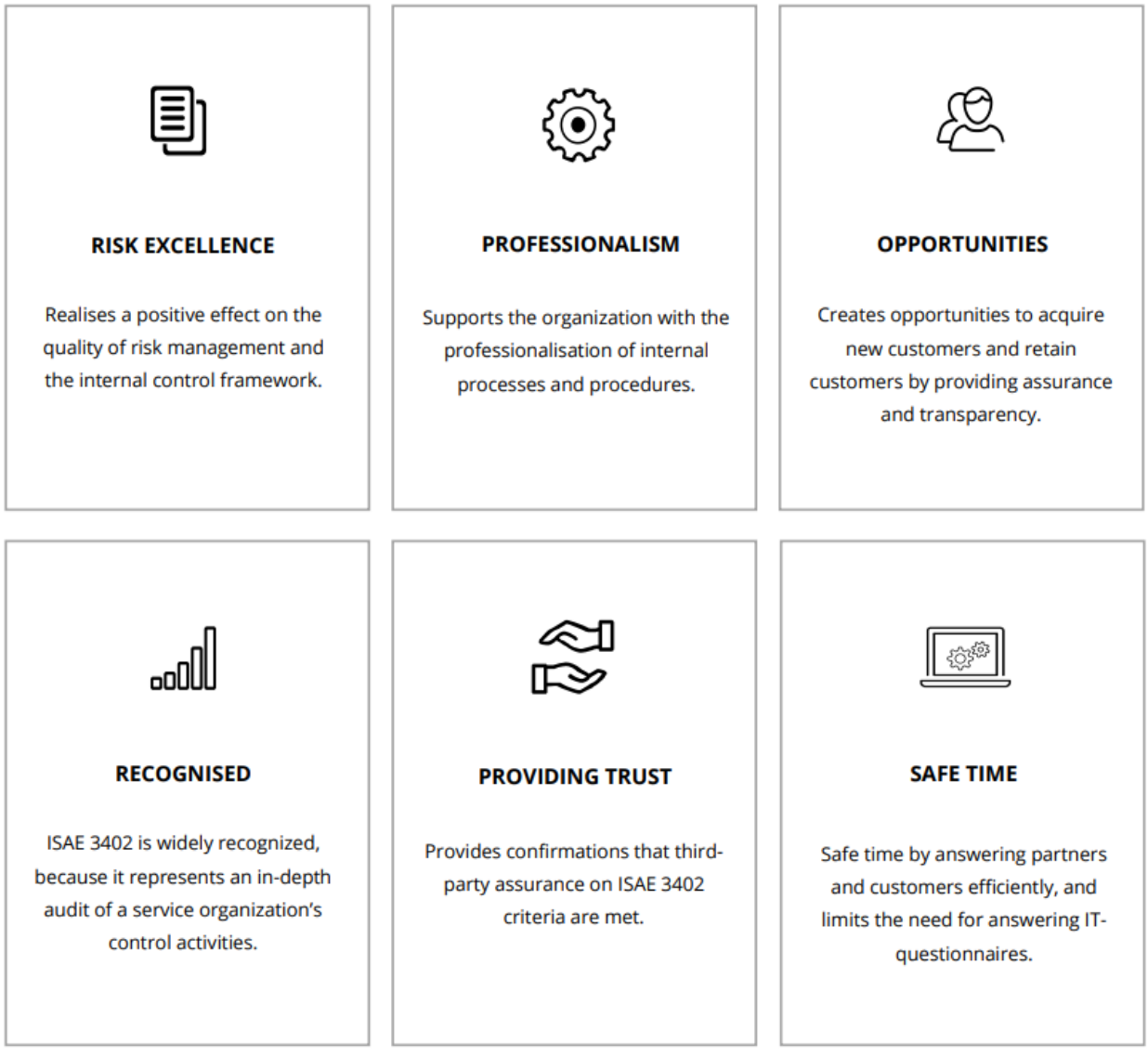


Nyckelfördelar

med ISAE 3402 -efterlevnad

Upplev födelarna med ISAE 3402-rapporter

ISAE 3402-rapporter används av organisationer som ett marknadsföringsverktyg. Nya och befintliga kunder inser direkt att de har att göra med en pålitlig part. Organisationer som inte har sådana rapporter kan gå miste om viktiga nya möjligheter. Under försäljningsprocessen är det vanligt att en kund ber sin leverantör att fylla i ett frågeformulär för att få insikt i organisationens nuvarande mognadsnivå. En ISAE 3402-rapport kan nu ge effektiva svar på dessa frågor och påskynda processen avsevärt. Detta ger också kunden en känsla av förtroende för att processerna verkligen är i ordning.



Introducerar Securance

Investera I effektivitet, värde och partnerskap

- **Analysera risker**
- **Planera projekt**
- **Förbered systembeskrivningar**
- **Utför en mognadsbedömning**

Att implementera ISAE 3402 kräver effektiv planering, ledningsengagemang, grundlig analys av processer samt pålitliga resurser och projektledning.

Securance härstammar från en av de "Big Four"-revisionsbyråerna och grundades 2004. Tack vare vår bakgrund arbetar vi enligt de högsta professionella standarderna och har erfarenhet av att arbeta med strama tidsramar. Vi lever upp till våra professionella standarder och levererar alltid högsta kvalitet, samtidigt som vi ständigt strävar efter att möta våra kunders behov.

Som en följd av vår platta struktur och effektiva kommunikationsram kan vi snabbt svara på dina behov. Att välja Securance innebär att välja en professionell organisation, men också att välja en personlig approach. Effektiv projektledning, vår erfarenhet av att implementera riskhanteringsramverk inom din bransch och professionalism är enligt oss grunden för utmärkta resultat.

På Securance tror vi att en god förståelse, tydlig kommunikation och kunskap om våra kunders branscher är avgörande för att leverera mervärde till dig som kund. Med denna approach kommer vi att hålla dig informerad om relevanta förändringar i lagar, regler och andra viktiga utvecklingar.
.

SECURANCE
BE SURE

Våra Nöjda Kunder

Referenser

SECURANCE
BE SURE

Securance Ltd.

63-66 Hatton Garden
London EC1N 8LE, UK
+44 20 351 446 56
www.securance.co.uk

Securance - Seadot

Sidenvävargatan 17
753 19 Uppsala
+46703040656
www.seadot.se

Securance BV

Reactorweg 47
3542 AD Utrecht
+31 (0)30 2800888
www.securance.nl